Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of the Claims:

1. (Currently Amended) A method comprising:

establishing a master secret between a first communications device and a second communications device;

sending a random access connection request burst from the first communication device to the second communications device;

opening a connection between the first communications device and the second communications device in response to the random access connection request burst;

~~generating a connection secret from the master secret~~

generating an initialization vector using an absolute frame number of the random access connection request burst;

determining a connection secret using the master secret and the initialization vector; and

using the connection secret for symmetric key cryptography during the connection.

2. (Original) The method of claim 1, wherein using the connection secret for symmetric key cryptography comprises:

initializing a cipher using the connection secret; and

sending one or more bursts over the connection, the one or more bursts carrying data encrypted using the initialized cipher.

3. (Original) The method of claim 1, wherein using the connection secret for symmetric key cryptography comprises:

initializing a cipher using the connection secret;

receiving one or more bursts over the connection, the one or more bursts carrying data encrypted using the initialized cipher; and

decrypting the data using the initialized cipher.

4. – 8. (Canceled)

9. (Currently Amended) The method of ~~claim 4~~ claim 1, wherein the first communications device does not sent the initialization vector to the second communications device.

10. (Canceled)

11. (Original) The method of claim 1, wherein the connection comprises a communications stream.

12. (Original) The method of claim 2, wherein the cipher comprises a stream cipher.

13. (Original) The method of claim 12, wherein the stream cipher comprises an RC4 cipher.

14. (Currently Amended) A communications device comprising:

a memory to store a master secret being known only by the communications device and a second communications device;

a secret generation module coupled to the memory to generate a connection secret from the master secret in response to the communications device opening a connection with the second communications device by generating an initialization vector using an absolute frame number of a random access connection request burst used to request the opening of the connection, and determining the connection secret using the master secret and the initialization vector; and

an symmetric key cryptography module to use the connection secret during the connection for symmetric key cryptography.

15. (Original) The communications device of claim 14, wherein the symmetric key cryptography module uses the connection secret as a symmetric key when encrypting data.

16. (Original) The communications device of claim 15, wherein the symmetric key cryptography module initializes a cipher with the connection secret.

17. (Original) The communications device of claim 15, further comprising a transmitter to send one or more bursts over the connection, the one or more bursts carrying data encrypted using the initialized cipher.

18. (Original) The communications device of claim 14, wherein the symmetric key cryptography module uses the connection secret as a symmetric key when decrypting encrypted data.

19. (Original) The communications device of claim 18, wherein the symmetric key cryptography module initializes a cipher with the connection secret.

20. (Original) The communications device of claim 15, further comprising a receiver to receive one or more bursts over the connection, the one or more bursts carrying the encrypted data.

21. – 25. (Canceled)

26. (Currently Amended) A machine-readable medium storing data representing instructions that, when executed by a processor of a first communications device, cause the processor to perform operations comprising:

establishing a master secret between the first communications device and a second communications device;

sending a random access connection request burst from the first communication device to the second communications device;

opening a connection between the first communications device and the second communications device in response to the random access connection request burst;

~~generating a connection secret from the master secret~~

generating an initialization vector using an absolute frame number of the random access connection request burst;

determining a connection secret using the master secret and the initialization vector; and

using the connection secret for symmetric key cryptography during the connection.

27. (Original) The machine-readable medium of claim 26, wherein using the connection secret for symmetric key cryptography comprises:

initializing a cipher using the connection secret; and

sending one or more bursts over the connection, the one or more bursts carrying data encrypted using the initialized cipher.

28. (Original) The machine-readable medium of claim 26, wherein using the connection secret for symmetric key cryptography comprises:

initializing a cipher using the connection secret;

receiving one or more bursts over the connection, the one or more bursts carrying data encrypted using the initialized cipher; and

decrypting the data using the initialized cipher.

29. – 33. (Canceled)

34. (Currently Amended) The machine-readable medium of claim ~~29~~ 26, wherein the first communications device does not sent the initialization vector to the second communications device.

35. (Canceled)

36. (Original) The machine-readable medium of claim 26, wherein the connection comprises a communications stream.

37. (Original) The machine-readable medium of claim 2, wherein the cipher comprises a stream cipher.